UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,659	06/25/2003	Bing Wang	08212/0200290-US0/NC28834	4744

38879 7590 03/07/2007

DARBY & DARBY P.C.
P.O. BOX 5257
NEW YORK, NY 10150-6257

EXAMINER	
HO, THOMAS M	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/606,659	WANG ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 are pending.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 17-25, 27-29 of the claimed invention is directed to non-statutory subject matter. Applicant's specification pgs 16, lines 21-23 indicate that the specified means or components may be implemented completely as software. Software is non-statutory subject matter under 35 USC 101 and must effect a change outside the system to be statutory.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4, 5, 14, 15, 21, 24 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are the steps required to perform a "rough outline hash value" and a "sophisticated signature hash value"

The Applicant has recited these two limitations in claims 3 and 4, respectively. However neither an "ROHV" nor a "SSHV" is a conventional term of art. Because of this, one of ordinary skill in the art of computer science would not know how to produce these two computations or values without details disclosing their essential elements and the steps required to produce them.

Claim 6 is additionally rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically claim 6 recites the method of claim 1, wherein immediately processing the object comprises not scanning the object. However the Examiner notes that processing an object in computer science inherently necessitates "scanning the object".

That is, if a computation or processing is performed on an object, the object must be read by the computer. "Scanning" is a term of art understood by those in the computer arts to mean "reading".

Additionally, the Examiner notes that the processing the object comes in reference to claim 1, where the processing is performed if the third value matches at least one of the values in the fourth set.

In this respect, the Examiner is aware of the Applicant's intention to provide a method of saving processing time from unnecessary virus scanning, particularly if it can be determined that the file in question was previously scanned. However, the Examiner notes that even this determination can be considered a form of "virus scanning." That is to say, broadly construed, determining where not to search may be considered as part of the process of "searching."

Claim 6 is not so indefinite as to preclude examination. Nevertheless, there are multiple interpretations to the meaning of the claim as set forth above. The Examiner requests the Applicant clarify the interpretation of the claim.

To expedite prosecution, the Examiner has interpreted claim 6 "without scanning the object" to not preclude "scanning to determine that no further virus scanning is necessary"

Claim Rejections - 35 USC § 102/103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 6-13, 16-20, 22-23, 25-29 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Chen et al. and the conventional art.

In reference to claim 1:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses a method for filtering out exploits passing through a device, comprising:

- Receiving an object directed to the device, where the object directed to the device is the virus scanning object, and where the device is the client. (Column 6, line 15-26)
- Determining a first value associated with the object, where the first value associated with the object is string A1 for virus A. (Column 13, line 24 – 37)
- Determining a second set of values associated with objects that have previously been scanned, where the second set of values are the set of virus strings: A1, A2, and A3, where the second set of values are the set of virus strings comprising virus string A which is associated with virus A (Figure 4d, 4b) and the set of virus strings have been previous scanned to determine that they are apart of the virus. (Column 13, line 1-37)
- If the first value matches at least one of the values in the second set, where a determination is made if the first value A1, matches one of the values in the second set. (Column 13, line 57 – Column 14, line 31)

- Determining a third value associated with the object, where the third value is virus string B1. (Column 13, line 24 – 37)
- Determining a fourth set of values associated with the objects that have previously been scanned, where the fourth set of values are the set of virus strings: B1, B2, and B3, where the fourth set of values are the set of virus strings comprising virus string B which is associated with virus B (Figure 4d, 4b) and the set of virus strings have been previous scanned to determine that they are apart of the virus. (Column 13, line 1-37)
- If the third value matches at least one of the values in the fourth set, immediately processing the object, where if the third value B1 matches one of the values in the set of B virus strings, the object is processed by producing an additional virus detection object. (Column 13, line 57 – Column 14, line 31)

In reference to claim 2:

Chen et al. (Column 7, lines 20-40) discloses the method of claim 1, wherein the object includes at least one of a message, an attachment to a message, an email, a computer-executable file, and a data file, where the virus detection object is an executable file and a data file.

In reference to claim 3:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & in particular (Column 13, line 24-37) discloses method of claim 1, wherein the at least one of the first value and the third value further comprises at least one of a hash value, an

algorithmic function, a checksum, a public key certificate, and a digital signature, where the first and third value, A1 and B1 comprise a digital signature, the "virus signature".

In reference to claim 6:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses the method of claim 1, wherein immediately processing the object further comprises processing the object without scanning the object, where the object is not scanned for virus C or any viruses who signatures portions being searched for were not found.

In reference to claim 7:

Chen et al. (Column 15, lines 35-55) discloses the method of claim 6, wherein immediately processing the object further comprises removing an exploit from the object, where the exploit that is removed is the virus.

In reference to claim 8:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & (Figure 2) discloses the method of claim 6, wherein immediately processing the object further comprises forwarding the object to a destination, where the object is forwarded to the server to determine if a second virus detection object needs to be transmitted.

In reference to claim 9:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses the method of claim 1, further comprising if the first value does not match any of the values in the second set,

- Scanning the object for an exploit, where the object is scanned for a virus exploit.
- Updating the second set of values to include the first value, where the second set of values A1, A2, A3, includes the first value A1. (Column 13, lines 24 – line 67)

In reference to claim 10:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses the method of claim 1, further comprising if the third value does not match any of the values in the fourth set,

Scanning the object for an exploit, where the object is scanned for a virus exploit

- Updating the fourth set of values to include the third value, where the fourth set of values B1, B2, B3, includes the third value B1. (Column 13, lines 24 – line 67)

In reference to claim 11:

Chen et al. (Column 5, lines 34-45) discloses the method is operable on at least one of a firewall, a router, a switch, a server, and a dedicated platform, where the system is operable on a client-server dedicated platform.

In reference to claim 12:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) & (Figure 4d) discloses the computer readable medium encoded with a data-structure, comprising:

- A first indexing data field having indexing entries, each indexing entry including a first value, where the first indexing entry includes the value of the virus sub-signatures. (Figure 4d)
- A second data field including object-related entries, each object-related entry having a second value and being indexed to an indexing entry in the first indexing data field, each object-related entry being uniquely associated with an object that has been previously scanned, where the second data fields comprise the composite virus signatures, and each virus object related entry is uniquely associated with the virus it identifies, and where these signatures were previously determined or "scanned" to match it with the virus it identifies. (Figure 4d)

In reference to claim 13:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & in particular (Column 13, line 24-37) discloses the computer-readable medium of claim 12, wherein at least one of the first value and the second value further comprises at least one of a hash value, an algorithmic function, checksum, public key certificate, and a digital signature, where the first and second set of values value, A1 and A comprise a digital signature, the "virus signature".

In reference to claim 16:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) & (Figure 4d) discloses the computer-readable medium of claim 12, wherein at least one object-related entry in the second data field includes information about the associated object, where the data in second data field includes signature information to identify a virus.

In reference to claim 17:

Chen et al. discloses a system for protecting a device against an exploit, comprising:

- A message tracker that is configured to determined whether an object has been previously scanned using a two-phase hash value technique, where the message tracker tracks down the virus detection object that is sent from the server to the client. (Column 6, lines 15-26), and where a determination is made to see if the object has been previously scanned using an iterative virus string detection technique. (Column 14, lines 13-63), and where the two phase hash value technique comprises the iterations of the virus signature string detection, and the determination of previously scanned necessarily occurs in the determination of whether another virus detection object need to be made and additional scanning is needed. (Figure 2, Item 245)
- A scanner component that is coupled to the message tracker and that is configured to receive an unscanned object and to determine whether the unscanned object includes an exploit, where the scanner component is coupled to the iterative virus detection module (Figure 4b)

In reference to claim 18:

Chen et al. (Column 7, lines 20-40) discloses the system of claim 17, wherein the object includes at least one of a message, an attachment to a message, an email, a computer-executable file, and a data file, where the virus detection object is an executable file and a data file.

In reference to claim 19:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & in particular (Column 13, line 24-37) discloses the system of claim 17, wherein the two-phase hash value technique comprises:

- Determining a first value associated with the object, where the first value associated with the object is string A1 for virus A. (Column 13, line 24 – 37)
- Determining a second set of values associated with objects that have previously been scanned, where the second set of values are the set of virus strings: A1, A2, and A3, where the second set of values are the set of virus strings comprising virus string A which is associated with virus A (Figure 4d, 4b) and the set of virus strings have been previous scanned to determine that they are apart of the virus. (Column 13, line 1-37)
- If the first value does not match at least one of the values in the second set, determining that the object has not been previously scanned, where a determination is made if the first value A1, matches one of the values in the second set. (Column 13, line 57 – Column 14, line 31)

In reference to claim 20:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & in particular (Column 13, line 24-37) discloses the system of claim 19, wherein the first value further comprises at least one of hash value, an algorithmic function, checksum, public key certificate, and a digital signature, where the first value, A1 comprise a digital signature, the "virus signature".

In reference to claim 22:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & in particular (Column 13, line 24-37) discloses the system of claim 19, wherein the two-phase hash value technique further comprises:

If the first value matches at least one of the values in the second set,

- Determining a third value associated with the object, where the third value is virus string B1. (Column 13, line 24 – 37)
- Determining a fourth set of values associated with the objects that have previously been scanned, where the fourth set of values are the set of virus strings: B1, B2, and B3, where the fourth set of values are the set of virus strings comprising virus string B which is associated with virus B (Figure 4d, 4b) and the set of virus strings have been previous scanned to determine that they are apart of the virus. (Column 13, line 1-37)
- If the third value does not match at least one of the values in the fourth set, determining that the object has not been previously scanned, where if the third

value B1 matches one the values in the set of B virus strings, the object is processed for viruses. (Column 13, line 57 – Column 14, line 31)

In reference to claim 23:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & in particular (Column 13, line 24-37) discloses the system of claim 22, wherein the third value further comprises at least one of a hash value, an algorithmic function, checksum, public key certificate, and a digital signature, where the third value, B1 comprise a digital signature, the "virus signature".

In reference to claim 25:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses the system of claim 22, wherein the two-phase hash value technique further comprises:

- If the third value approximately matches at least one of the values in the fourth set, determining that the object has been previously scanned, where if string B1 matches one of the values in the B set of strings, it can be determined that the object has been previously scanned in that a determination has also been made to see if the object has virus string A or virus string C within it. (Column 13, line 55 – Column 14, line 30)

In reference to claim 26:

Chen et al. (Column 5, lines 34-45) discloses the system of claim 17, wherein the system is operable on at least one of a firewall, a router, a switch, a server, and dedicated platform, where the system is operable on a client-server dedicated platform.

In reference to claim 27:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses the apparatus for protecting a device against an exploit, comprising:

- Means for receiving an object directed to the device, where the device is the client, and the client receives the virus detection object from the server (Column 6, lines 15-26)
- Means for determining whether the object has been previously scanned using a two-phase hash value technique, where the message tracker tracks down the virus detection object that is sent from the server to the client. (Column 6, lines 15-26), and where a determination is made to see if the object has been previously scanned using an iterative virus string detection technique. (Column 14, lines 13-63), and where the two phase hash value technique comprises the iterations of the virus signature string detection, and the determination of previously scanned necessarily occurs in the determination of whether another virus detection object need to be made and additional scanning is needed. (Figure 2, Item 245)
- Means for immediately processing the object if the object has been previously scanned, where the object is processed in that the server produces a vaccine based on the reported results of the virus detection object. (Figure 2, Item 255)

In reference to claim 28:

Chen et al. (Figure 2, Item 210) discloses the apparatus of claim 27, further comprising means for scanning the object if the object has not been previously scanned.

In reference to claim 29:

Chen et al. (Figures 4b, 4c, 4d) apparatus of claim 27, further comprising:

- Means for maintaining a list of previously scanned objects for the two-phase hash value technique, where the list of previously scanned objects for the two phase hash value technique includes the virus signature string data, and the virus data characteristics. (Figures 4d, and 4c respectively)
- Means for updating the list, where Chen et al. discloses a means for updating the list as a conventional method in the art. (Column 1, lines 34-52)

Conclusion

6. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on **(571)272-3799.**

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

Feburary 26th, 2007

Thomas Ho 10 2132

Benjamin E. Lanier
Examiner AU 2132